REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
25-04-2013

2. REPORT TYPE
Master of Military Studies Research Paper

3. DATES COVERED *(From - To)*
September 2012 - April 2013

4. TITLE AND SUBTITLE
Unified Communications: Simplifying DoD Communication Methods

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Holmes, Eric, L., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

The current methods of transmitting information are at times not suitable for a commander's need for the relay of mission-critical information in near real-time. Unified communications technology is able to deliver the flexibility and adaptability required to provide reliable and expedited communications to forces in distributed austere environments. Unified communications enables users to link applications into a common user interface facilitating collaboration on enterprise networks and across the Global Information Grid (GIG). Reporting time-sensitive information or responding to commander's critical information requirements (CCIRs) is vital at all levels of warfare, but it is particularly important at the operational level. At the operational level commanders lead forces that are dispersed across significant time and space. Having the ability to host impromptu meetings and coordinate efforts is essential to maintaining a high operational tempo. The military operates in a fast paced environment where the reliable and expedited exchange of information is crucial to mission success. Unified communications will help the military to make better use of existing capabilities and enhance staff effectiveness.

15. SUBJECT TERMS
Unified Communication, IM, Presence, Conferencing

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Marine Corps University/Command a
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	70	**19b. TELEPHONE NUMBER** *(include area code)*
Unclass	Unclass	Unclass			(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Unified Communications: Simplifying DoD Communication Methods

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Major Eric L Holmes

AY 12-13

Mentor and Oral Defense Committee Member: MATTHEW FLYNN
Approved:
Date: 4/18/13

Oral Defense Committee Member: J.W. Gordon
Approved:
Date: 4/18/13

CDR USN
MILFAC/CG-4
4/18/13

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

Page

Illustrations

Preface

This paper addresses a need within the US military for embracing and integrating existing communication technology. As a communications officer in the United States Marine Corps, I am responsible for the design, installation, operation, and maintenance of communication architectures. The United States military is considered the most technologically advanced military in the world, yet it uses communications equipment decades outdated and software years behind the industry standard. The Department of Defense places obstacles in its path to efficiency. Each service maintains its network independently. Each network is designed in similar fashion and yet has little to no interoperability. It has only recently become possible to email a person in the Navy from a Marine Corps Exchange client, although both services are under the same department. These silos of excellence, as I refer to them in this study, are inhibitors to efficiency and collaboration, a key weakness in any organization but even more so in a military organization. While I do not claim to have all the answers I do believe that researching and testing potential solutions is better than the status quo.

I would like to thank my academic mentor for his guidance on changing my topic to one more appropriate to my interests. I would also like to thank him for his understanding as I worked through some difficult personal issues. I would also like to thank all of my proof readers, and there were many. Without your help I would probably have had a lot more typos. Finally I would like to thank everyone from Microsoft who took time out of their busy schedules to help me track down valuable research and even volunteered to provide feedback on my paper.

Executive Summary

Title: Unified Communications: Simplifying DoD Communication Methods

Author: Major Eric L Holmes, United States Marine Corps

Thesis: The implementation of unified communications will provide the Department of Defense with an interoperable communications platform across disparate systems that will effectively increase the warfighter's ability to make decisions.

Discussion: The current methods of transmitting information are at times not suitable for a commander's need for the relay of mission-critical information in near real-time. Unified communications technology is able to deliver the flexibility and adaptability required to provide reliable and expedited communications to forces in distributed austere environments. Unified communications enables users to link applications into a common user interface facilitating collaboration on enterprise networks and across the Global Information Grid (GIG).

Conclusion: Reporting time-sensitive information or responding to commander's critical information requirements (CCIRs) is vital at all levels of warfare, but it is particularly important at the operational level. At the operational level commanders lead forces that are dispersed across significant time and space. Having the ability to host impromptu meetings and coordinate efforts is essential to maintaining a high operational tempo. The military operates in a fast paced environment where the reliable and expedited exchange of information is crucial to mission success. Unified communications will help the military to make better use of existing capabilities and enhance staff effectiveness.

Introduction:

The United States Department of Defense (DoD) utilizes various forms of communication to command and control operational forces and direct the day-to-day functions of garrison units. The DoD has not experienced an inability to communicate nor a detrimental degrade in communication functions that have prohibited the effective command and control of operational forces. This does not mean there is not a more effective way of employing the technology the DoD has available. Unified Communications (UC) is a technological capability that facilitates the integration of multiple communication mediums. The use of UC can enhance communication between joint and or coalition forces making existing communication mediums seamless to the end user. The implementation of UC will provide the DoD with an interoperable communications platform across disparate systems that will effectively increase the warfighter's ability to make decisions.

Digital communications changed the way the services operate on the battlefield and in garrison. Inter and intra networking architectures have made the exchange of information between distributed forces a simple process. Electronic mail (email), instant messaging (IM), and video conferencing aid the ability of service members to be productive regardless of where they are located or who they are collaborating with. However, the current system platforms function as "silos" which do not allow for flexible real time communications. UC can bridge the gap between platforms and facilitate seamless real time communications. Ultimately, overcoming any large organization's tendency to compartmentalize is essential, something DoD has addressed overtly for some time. Now is the time to take the step and to do so with UC.

Literature Review:

UC is a pivotal part of any plan to consolidate redundancy in IT system deployments. The majority of professional literature on UC speaks to the benefits of a successful implementation in business. Bern Elliot's article, *The Value of Unified Communications*, suggests effective employment of UC will make businesses more agile and responsive. The DoD can benefit from improvements in both of these areas. Elliot goes on to argue that the use of *presence* is crucial to an organization's ability to streamline processes. Elliot concludes that *presence* enables users to identify the appropriate individuals within an organization to address problems.

The examples provided in Neeraj Gill's article, *Putting the Unified in Unified Communications-Collaboration is the Key*, address the improvements gained through the use of UC capabilities. Gill suggests that the efficiencies UC provides will make business communications seamless, instantaneous, and cost-effective. Like Elliot, Gill proposes that UC will make businesses more responsive.

There is a common theme throughout the literature on UC. That theme is the importance of presence to UC. *Presence* is the foundation of a well-developed UC architecture. Roger Hulme's article, *One for all: Unified Messaging Comes of Age,* describes presence as an essential element of UC. *Presence* allows users to know who is available and by what means they can be reached. This enables the business to be more effective. Thus UC aids a business in being agile and responsive. The ability to effectively command and control forces on a distributed battlefield requires commanders and staff members at the operational level to be responsive. One can gather from the literature that UC is ideal for command and control.

UC is not a perfect solution. Critics of UC highlight security and privacy vulnerabilities to both personal and corporate information. Jun Xu's article, "E-Business in the 21st Century: Realities, Challenges and Outlook, concludes that system integration will be a major issue for most adopters of UC. However," he goes on to state that if UC is successfully integrated, businesses will see significant Return on Investment (ROI). It is clear that even critics see the benefits of UC if implemented properly.

The literature on UC is sparse. The limited coverage detailed above represents much of the expertise addressing this topic. There are, of course, technical manuals that do the obvious: they allow configuration of UC so the user can maximize its potential, but no more. The conceptual benefit, particularly going from a business to a military organization is not addressed. This MMS begins this conversation.

DoD Digital Communications, Background:

Senior leaders within the US military have grown accustomed to working in a digital environment. Leaders who entered service prior to 1990 can be referred to as digital immigrants. They are seen as digital immigrants because they adapt analog processes and learn to operate in the digital environment. Digital immigrants are able to navigate volumes of data, exchange crucial information, and draft reports in a fraction of the time possible a few years ago. However, digital natives have shown that they are capable of processing information and collaborate at a rate previously thought impossible. A digital native is "a person born or brought up during the age of digital technology and so familiar with computers and the Internet from an early age."[1] There is nothing physically different between digital natives and digital immigrants. The difference between digital natives and digital immigrants is how they think about and process information.

A digital immigrant is more likely to print a document and edit the hard copy instead of editing the digital version using built in tracking or comment features within the application.[2] "Digital natives are used to receiving information really fast. They like to parallel process and multi-task," says Marc Prensky, an expert in the field of education and learning.[3] Understanding the differences between digital users is significant because the current non-commissioned officers and junior officers are digital natives. All new recruits and commissioned officers going forward will be digital natives. Digital natives not only are willing to embrace new technology, they demand that these technologies are made available to use to their advantage. The use of social networking as a collaborative medium is a primary example.

Social media is a powerful example of UC in action. Users of social media are capable of knowing who is available online and what forms of communication (email, IM, voice) is accessible to the other users at a glance. The user is able to reach a colleague in the most appropriate form given the associate's online status. Another benefit of UC's integration into social media is platform ubiquitous delivery of information. A person could be at their desk on a computer, in a meeting using a tablet, or outside the building using their mobile phone and still have the message routed to the correct device.

Social media is a perfect example of integrating the communication medium. The DoD has mandated that social media sites be accessible from DoD networks. In February of 2010 the DoD released Directive-Type Memorandum (DTM) 09-026, titled *Responsible and Effective use of Internet-based Capabilities.* The purpose of DTM 09-026 is as follows:

> This memorandum establishes DoD policy and assigns responsibilities for responsible and effective use of Internet-based capabilities, including social networking services (SNS). This policy recognizes that Internet-based capabilities are integral to operations across the Department of Defense.[4]

In response to DTM 09-026 the Marine Corps released Marine Administrative Message (MARADMIN) 181/10. MARADMIN 181/10, titled *Responsible and Effective Use of Internet-based Capabilities,* reversed the Marine Corps ban on the use of SNS on the Marine Corps Enterprise Network (MCEN). MARADMIN 181/10 did not open up the network to all SNS. It also established restrictions on when and the duration SNS could be accessed from machines on the MCEN.[5]

The use of SNS to share For Official Use Only (FOUO) material is strictly prohibited. The user agreement statements associated with SNS clearly states that the material posted to the site becomes the property of the site and can be used for any purpose. When establishing an account on Facebook users must agree to Facebook's

Statement of Rights and Responsibilities. In the *Statement of Rights and Responsibilities* it says the following:

> Content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.[6]

Deliberately giving up control of FOUO information/material is in direct violation of the Marine Corps Operations Security (OPSEC) Program. Therefore, SNS are not suitable for DoD collaboration. This does not negate the fact that a means of collaboration is needed. UC fills this need. The protection of government information is paramount in network security. Because of stringent network defense requirements for DoD infrastructure UC solutions must be tightly controlled. The safeguarding of DoD information takes precedence to ease of use. Employed correctly a UC solution can facilitate cross boundary communications that is both government controlled and secure. A UC solution of this type could support all services, government agencies, and coalition forces.

The potential UC represents for collaboration and work productivity is limitless. There are some security concerns that must be addressed for deployment on the DoD network; however, any full scale enterprise employment of a platform would need to address similar concerns. UC will offer service members a "streamlined mechanism for managing communications. The user could check all message types, regardless of communication device, from one central location."[7] The deployment of UC will deliver unparalleled collaborative capabilities compared to the DoD's current network architecture. It is essential that a UC system expand beyond the current service boundaries. An effective DoD level enterprise collaboration medium does not exist. The lack of integration at the DoD level hinders information exchange between units of different services. This limitation affects operational level planning and decision making.

What is Unified Communications:

It is important to define UC in order to understand the benefits it provides. A UC platform can consist of a multitude of integrated software features. According to Bern Elliot, the lead Gartner analysis in unified communication, states:

> elements of unified communications include VoIP systems, e-mail, audio and Web conferencing, videoconferencing, voice mail, unified messaging and IM. These are evolving toward integration, but each also is developing in its own way. For instance, voice, video and Web conferencing capabilities will converge, and IM's presence capabilities will expand to all live channels, including voice, conferencing, video and e-mail.[8]

It is apparent that experts in the field view converging technology as the next step in the evolution of information systems. Merging voice with data or email with voicemail provides users with the means to maintain constant connectivity. Commanders can theoretically command and control from one mobile device.

A good UC platform will consist of four key features: voice, email, conferencing, and instant messaging/presence. By integrating these features UC provides the framework for a more efficient collaborative environment in which the various communication mediums become an enabler to productivity.

Voice: A Voice system is the most important communication capability. The telephone is the primary form of communication for many users. From its inception through today it has continued to be a vital part of any organization. Telephone systems are a network of connected circuit switches. Those circuit switches are referred to as the Public Switched Telephone Network (PSTN). Most users connect to a PSTN for access; however, large organizations sometimes have a need for a robust internal phone network.[9]

Like many large organizations the enterprise voice systems within the Marine Corps are legacy private branch exchange (PBX) based voice systems. However, many are transitioning to

Internet Protocol (IP) based voice systems. IP based phone systems are quickly replacing traditional phone lines. Voice over IP (VoIP) phones offer organizations significant cost savings over traditional phone lines. There is a downside to VoIP phones. If there is a network outage VoIP phones will not work. Another issue is bandwidth. If the amount of bandwidth available reduces, VoIP calls will experience degradation. The quality of the call will continue to degrade in relation to the amount of bandwidth available until the call drops. For system redundancy a degree of traditional PBX need to remain online allowing for a hybrid IP/PBX architecture that will allow for integration into a larger suite of interconnected communication systems while maintaining reliable connectivity if there is a network system outage.

The incorporation of tactical voice communication into a UC architecture is pivotal for deployed forces. The introduction of Radio over IP technology has made communication with dispersed forces easier. RoIP is similar to VoIP except the data signal is transmitted to a tactical radio unit. The current RoIP technology is capable of facilitating UC in the field. By integrating UC at the tactical level commanders can close the gap on reporting of significant events.

Email: Service members and civilians within DoD rely heavily on email as a means of conducting business. It is a requirement for an email client to support assured delivery. Next to the telephone, email is the most widely used form of communication within most organizations. In fact, in some instances email may be the primary form of communication. What makes email so valuable is it allows users to communicate at their convenience. Regardless of time differences or schedules one could send an email and wait for a response.

An additional benefit of email is the ability to address multiple recipients. Most phone bridges have a maximum capacity of 20 callers; however, an email can be addressed to a limit of 500 recipients.[10] The Marine Corps currently deploys Microsoft Exchange email server. The fact that the Marine Corps has already deployed Exchange as an enterprise email solution will facilitate the ease of UC integration.

Conferencing: Some form of conferencing is used by most organizations. As budgets are reduced organizations are embracing web conferencing. The Marine Corps is no exception. There are currently two forms of Video Teleconferencing (VTC) systems within the Marine Corps. They are both Tandberg telepresence platforms. One is a desktop version; the other is a conference room suite system. Both are expensive. UC provides the opportunity to not only incorporate these systems into a more robust communication capability, but it will also allow for the deployment of cost effective video conferencing to countless additional users. Under current budget constraints low cost web cameras can replace expensive VTC suites. Shifting from dedicated VTC suites to a desktop camera integrated into a UC system could save millions.

Instant Messaging and Presence: The final minimum requirement includes an instant messaging capability with support for presence. IM is a common placed communication medium. Windows Live Messenger, Yahoo messenger, and Google Talk are excellent examples of commercially available IM clients. IM is a communication session established between one or more users. IM is considered a good mix between voice and email. Because IM is a live session it offers the immediate communication of a phone call while maintaining a written record like an email. This is one reason why military operation centers use IM for their reporting capability.

Presence is a lesser known network capability. Presence refers to a systems ability to display the current status of a user on the network. A simple way to think of presence is the status icon on an IM client. A green status symbol would indicate one is available. A red status symbol would indicate a user is in a meeting or away from their desk. When integrated into a UC platform presence becomes more useful than just displaying status. Presence can be fully integrated into calendar and voice features. The result would be a reactive system that would be independent of user input unless needed. An example would be if/when a user picks up the phone to make a call the presence status changes to show they are on the phone. Another example would be at the scheduled time of a meeting the user's presence status changes to reflect the meeting.

Microsoft offers one of the most complete UC platforms on the market to date. Microsoft's platform is Lync, which replaced Office Communication Server. Lync integrates IM, voice and video calling, online meeting, and application sharing into a single client offering.[11] Discussing the Microsoft Suite of office products presents an opportunity to provide a real world example of how UC works. Utilizing Microsoft Office and SharePoint users are able to share information. A user can create a document in Word then post that document to SharePoint. Other users can access this document and work on it simultaneously. These users can see the edits made by the other users accessing the document at the same time. If a question arises they can start an IM session with one or multiple users. If required, the users can escalate the session to a voice or video conference. In addition, if there is a contributor that is not online at the moment that person can be added regardless of location if that user is available.[12] This example is a significant improvement over the current capabilities available. Currently there is no way to determine if a contributor is online. Coordinating a meeting, phone conference, or VTC is the only way to bring coworkers together. This method does not guarantee all required participants will be available to attend. Through UC each participant can join the meeting via the best medium available to them.

Keeping with the example of Microsoft Lync as a UC platform, the use of a UC system can have tremendous telephony benefits. Integrating Lync with existing PBX IT managers can replace traditional desktop phones with VoIP softphones. The user will be able to make and receive calls from a desktop or laptop, significantly reducing hardware cost and access charges. Users with a requirement for reliable phone service can be equipped with a hardware based VoIP phone that can switch to the PBX if a network outage is experienced. Integrating the systems with a UC server allows the user to become mobile and yet still remain connected and productive. Calls are routed to the user's device based on the user's presence status. In addition, if a device with a front facing camera is available the user can participate in a video conference from anywhere.[13] This capability will give commanders the ability to be available at all times.

Unified Communications Vulnerabilities:

Some opponents of UC argue that the more integrated systems become the easier it will be to exploit potential vulnerabilities. A UC platform must be interconnected to operate with other systems. Once systems are connected they become susceptible to exploitations it was previously isolated from. Like civilian corporate networks DoD systems are built upon the following:

> network and application services that provide access to a variety of data sources. A perpetrator needs only a single weakness in order to attack a system. While some attacks require sophisticated techniques and technologies (i.e., denial of services, phishing, malicious software, hacking), most attacks are not sophisticated (i.e., preying on poor security practice and human weaknesses, social engineering)." Users of network systems are often oblivious to potential threats. Information technology (IT) managers have a better perspective on the risks associated with integrated systems.[14]

Gavin Hill, technology director at Dimension Data, conducted a survey of IT users and IT managers. Those surveyed covered a wide degree of experience levels. The survey found that 52% of IT users believed that unified communications technology was as secure as any other network system.[15] The IT managers surveyed were more skeptical of the security of UC. The survey found that only 31% of IT managers believed UC was as secure as any other network system.[16] These statistics indicate that most users give little consideration to security. Therefore, security needs to be built into the architecture at the design phase. However, the end user still has a responsibility to follow security protocols. The adoption of UC increases the number of attack vectors a hacker can infiltrate a network. If an organization implements UC both IT users and managers will need to adjust how they view cyber security.

The occurrence of cyber incidents on networks has increased at an alarming rate over the past several years.[17] John Rittinghouse, senior security and management executive at

Hypersecurity, claims that government and civilian "organizations continue to experience various cyber-attacks from inside and outside of the organization."[18] The DoD is a constant target for cyber-attacks that threaten operational networks daily. Some reports suggest that as many as 20,000 new malicious viruses are developed each day.[19] According to Dr. Talal Al-Kharobi and Mohmmed Abduallah Al-Mehdhar, the most effective attack against a UC suite is a distributed denial of service (DDOS) attack. A DDOS "attack works by sending a lot of strange, malformed or other types of packets to a server or gateway, and then the huge traffic is redirected to the victim node to make it stop responding."[20] The result of a DDOS attack could shut down IP services for any organization. According to J. Dawkins, CEO and founder of True Digital Security, DDOS attacks "target a host but impact the structure of the network, and attacks exploiting the structure of the network" can disrupt all services for that organization.[21]

Email and instant messaging face similar challenges. They both facilitate the effective exchange of information; however, they are both susceptible to interception. In the instance of email and IM the most common vulnerability is the user. Hackers utilize social engineering and spear phishing attempts to collect information on the user.[22] What is not discussed is how most exploits are initiated by the end user. Most viruses can be detected through normal scans. However, end users frequently open attachments without scanning, even when they do not know the origin exposing the machine and the network.

The benefit of current IP based conferencing systems is their multifaceted functionality. The DoD utilizes Defense Connect Online (DCO) for IP based conferencing. Within the DCO web application users can view video, hear audio, exchange documents, and share their desktops. Web conferencing consumes large amounts of bandwidth in order to establish and maintain a connection. A small drop in packets can have significant impact on a video conference call. This is evident by a jerky or frozen image even when the audio has not been interrupted. Web conferencing applications require a substantial amount of bandwidth. The large demand for capacity by web conferencing applications means any degradation in bandwidth would have a corresponding reduction of service reliability. A DDOS attack would be the most detrimental cyber threat to UC service.

Vulnerability Mitigation:

The writers that express concern over the vulnerability of UC fail to take into account basic network security practices. Although the threat is real, steps are taken to mitigate the risks. Each of the primary features of UC can be protected from exploitation. Distributed denial of service can have a significant impact on VoIP services. To maintain reliable service VoIP transmissions pass large amounts of data.[23] If there is a disruption of the data flow the user will experience an immediate drop in call quality. Employing sound network defense strategies will protect the network from attacks that can cripple not only UC but basic network services as well.

Zero day vulnerabilities are unknown and thus cannot be planned for. However, security for the network, and thus the systems operating on that network, can be taken into consideration and included in the network design. The development of a network security strategy must begin during the system analysis phase.[24] During the system analysis phase IT administrators must determine the types of Internet traffic necessary to complete the organization's mission. Once the type of traffic permissible is identified administrators can create an access control policy[25] "An access control policy is simply a corporate policy that states which type of access is allowed across an organization's network perimeters. For example, your organization may have a policy that states, 'Our internal users can access Internet websites and FTP sites or send SMTP mail, but we will only allow inbound SMTP mail from the Internet to our internal network.'"[26] The access control policy is the foundation for safeguarding UC systems on the network. The early identification of accepted network traffic allows administrators to screen for and block anything outside of the approved parameters.

By taking into account the security considerations for UC before a deployment IT managers can save time, resources, and money. While UC offers benefits it also presents a unique set of challenges. For example, when voice systems are integrated with the data network the two separate systems security vulnerabilities are capable of crossing boundaries. Issues such as this one must be considered during the planning and system analysis phase.

The first line of defense for an enterprise network is the Demilitarized Zone (DMZ). The DMZ consists of external and internal facing firewalls as well as servers. All traffic that is passed to the internal intranet is filtered through the servers in the DMZ. Firewalls separate the DMZ from both the Internet and the organizations internal network. The purpose of a firewalls programming is to enforce the access control policies developed during the system analysis phase. The IT administrator is able to control the level of connectivity through the firewall. Once the level of connectivity is determined the firewall ensures that access beyond those parameters is restricted.[27] The restriction of access beyond what is specified in the access control policy reduces the networks exposure to threats.

Firewalls generally utilize a combination of defensive measures to prevent intrusion. The most common measures are static packet filtering, dynamic packet filtering, and proxy.[28] Marine Corps firewalls use a combination of these features to form a defense in depth and minimize exposure. In order to understand the strengths and weakness of each they will be covered here.

Static packet filtering can be employed in order to control access to what enters and exits a network. "Static packet filtering controls traffic by using information stored within the packet headers. As packets are received by the filtering device, the attributes of the data stored within the packet headers are compared against the access control policy (referred to as an access control list [ACL])." [29] Once the packets are analyzed the firewall can make the determination to pass the packets through or block them.[30] Although static packet filtering is very efficient there are drawbacks to its usage. Static packet filtering only inspects the packet. The process happens at a fraction of a second; however, nothing is stored for future reference. This is significant because a hacker who codes a virus to appear as if it is a return request will infiltrate the firewall.

Because there are limitations to the efficiency of static packet filtering administrators may opt to utilize dynamic packet filtering. "Dynamic packet filtering takes static packet filtering one step further by maintaining a connection table in order to monitor the state of a communication session."[31] Having the ability to maintain a connection table allows the firewall to effectively screen sessions instead of only relying on the packet itself. The end result is better security with little intrusion on the end user's experience.

Analyzing how dynamic packet filtering handles attacks compared to static packet filtering reveals the effectiveness of the process. A common tactic of hackers is to send a packet that looks like it was requested by a system on the network. A static packet filter will analyze the packet and discover it contains an acknowledgment. The acknowledgment tricks the filter into believing the packet is a response to a request by a machine on the network. In this example the packet would be allowed to pass through the firewall. A dynamic packet filter cannot be fooled in this manner because it utilizes a connection table to identify active connections originated on the Local Area Network (LAN). "When the information is received, the dynamic packet filter references its connection table (sometimes referred to as a state table). When reviewing the table entries, the dynamic packet filter realizes that the internal system never actually connected to this external system to place a data request."[32] Because the information request did not originate on the LAN the packets are blocked from entering.

The establishment of a proxy server would prevent machines on the LAN from connecting directly to outside sources. A proxy, like its name implies, acts as a middleman for computers requesting information. The requesting machine would establish a connection to the proxy. In turn the proxy then establishes a connection outside the DMZ and requests the information. Because the internal machine never establishes the connection all the way through the DMZ its exposure is reduced.[33]

The combination of the previously mentioned security practices is the basis for an Intrusion Detection System (IDS). IDS does not only scan and analyze network traffic it also scans “access logs and analyzing the characteristics of files to see if they have been compromised.”[34] When security parameters are clearly set an IDS is capable of identifying and isolating anomalies on the network. Once quarantined the network intrusion can be eliminated.

Another form of network security is the use of a virtual private network (VPN). The use of a VPN would allow users to access corporate data while encrypting traffic.[35] “In the creation of a VPN connection, several security features come into play. These features include authorization, authentication, filtering, and encryption. Any organization considering implementing a VPN must take each of these features into account during its planning process.”[36] A VPN can be thought of as a tunnel. In fact, it is often referred to as tunneling. A secure network connection is established within public network traffic. Before a VPN is established the end-user must be authenticated thus ensuring unauthorized users do not gain access to the LAN. A commander or staff member can securely log onto the DoD network from any location with Internet access.

Another layer of protection would include the use of token-based access. A form of token-based access is Public Key Infrastructure (PKI). The DoD employs PKI as a way to digitally sign and encrypt emails as well as controlling access to restricted sites. PKI uses a combination of public and private keys for encryption and decryption[37] The DoD employs credentials on common access cards (CAC) for this process. When digitally signing emails the credentials on the CAC “creates a one-way hash of the data, and then uses the private key to encrypt the hash. The encrypted hash, together with some other information, such as the hashing algorithm, is known as a digital signature. In order to validate the integrity of the data, the receiving software first uses the signer's public key to decrypt the hash. It then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data."[38] Once the hash is verified the email is considered authentic. The use of a CAC to access the network, access restricted websites sites, and digitally signing emails provides a reasonable level of security for unclassified networks. Information that would require additional security would be moved to a classified network.

The network security policies and practices outlined in this section demonstrate the defense in-depth mentality of network security. While no one security feature is perfect the combination of multiple forms of security minimizes the weakness of any one system. A result of integrating network systems is an increase in potential vulnerabilities. The unified systems will be exposed to threats that it was previously isolated from. However, a robust network defense strategy designed and implemented responsibly will mitigate most if not all of the risk associated with UC. The issues identified are threats to networks systems irrespective of a UC deployment.

Benefits of Unified Communications:

A cultural shift must take place in order to convince leaders to see beyond service requirements and move toward the employment of a UC plan integrated at the DoD level. The DoD Unified Capabilities Master Plan (UCMP) is a good first step. The UCMP identifies the enablement of "strategic, tactical, classified and multinational missions with a broad range of interoperable and secure capabilities for converged non-assured and assured voice, video, and data services from the end device, through Local Area Networks (LANs), and across the backbone networks" as a significant benefit.[39]

On today's rapidly changing battlefield leaders need to have the ability to respond quickly to new information and make the appropriate decision. The communication systems deployed in support of our forces are increasingly more complex. Despite the investments made in the latest technology ensuring that the right information, is received by the right person, in a time frame that it is actionable is still difficult to achieve. The intent behind the DoD UCMP is to facilitate the warfighter's ability to maintain the initiative and aid leaders in making informed decisions.

The military's current budget constraints will require leaders to make a decision on maintaining the status quo or force closer cooperation and integration. The former will eventually lead to a technological lag in the communication systems of the services. With less money the services will be forced to "make do" with what is in the current inventory. Outdated communication assets will introduce vulnerabilities prime for exploitation. The latter will improve collaboration ensuring a truly joint common operational picture. The integration of systems will facilitate the utilization of shared resources. The sharing of resources will alleviate a single service the burden of funding new technology. An inter-service communication integration plan will save tax dollars and improve both operational and tactical level coordination. UC is the key to truly joint operations.

UC is a maturing technology that is rapidly gaining acceptance. As leaders and IT managers determine where UC fits in command and control the focus needs to shift from the technology itself to where UC solutions offer the most value.[40] Individuals have always managed to reach the appropriate person or deliver the right message to the intended recipient. However, it has not always been done as efficiently as possible. How many hours are spent trying to track down the right person? How much time is wasted trying to schedule the right people for a conference call? What opportunity was missed at the tactical level because the right decision make could not be reached?

In the business world, the military, and private life people have used phones, email, fax, and instant messaging to communicate. What makes unified communication an improvement over the way communication methods are currently conducted? What is the value added that makes UC worth the investment? The simplest feature of UC is the most impactful. The presence feature is what starts to bind the other features together and make them force multipliers. Presence is what truly distinguishes UC from other methods of communicating. “Unified communications is designed to eliminate barriers that have traditionally separated voice calls, e-mail, instant messaging and conferencing in all forms.”[41] Presence will speed up the decision making process. Presence will allow a user to know what key decision makers are available at a glance. Being able to receive timely information and make decisions based off of that information will significantly reduce the cycles of the Observe, Orient, Decide, Act (OODA) loop.

Presence is what makes UC truly transformational. By establishing a common integrated platform it is possible to transition between devices seamlessly while maintaining connectivity and make availability known. Bern Elliot, lead analyst in UC with Gartner writes that “in addition to integrating communication channels…unified communications offers a way to integrate communication functions directly into business applications.”[42] This idea is like the example given earlier about phone or calendar integration. By having presence integrated into business applications users will know if you are available and by what means you are available. Elliot refers to this capability as “communications-enabled business processes (CEBP). By 2012, 80% of leading organizations will have adopted some form of CEBPs for competitive improvement.”[43]

UC brings together various mediums of communication technology providing the user with a simplified process for contacting other users. The intent is to reduce the difficulty of reaching a user by multiple means. Sending an email, sending a text message, and leaving a voicemail just to ensure the intended recipient receives the message is inefficient. UC cuts through these duplicative efforts allowing a user to send one message through any medium of their choosing with the certainty that the recipient will receive the message on the medium of their choosing. This process is more effective and breaks "down the barriers between voice, video, email, and other applications to improve communication and collaboration across enterprises."[44]

One of the most difficult things to do is work on an operational planning team (OPT) or a working group (WG). When assigned to one of these groups it is seldom ones only responsibility. Action officers in the Pentagon often find themselves assigned to several of these groups, some of which meet at the same time. This makes effective collaboration difficult if not impossible. UC can facilitate action officers' ability to participate on multiple groups by running different sessions on their desktop concurrently. Another problem with working groups is tracking down participants after the meeting adjourns. If a need arises for input on a crucial issue and the key decision maker is away from their desk the current forms of communication only allow one to leave a message, send an email, or send a text. All of these methods are not time sensitive. UC integration would allow one of those messages to be pushed to the device the user has with them. Team members also find it difficult to schedule impromptu meetings as complicated issues come up. "Trying to schedule informal or unplanned conference calls often results in delays while waiting for others to respond. Unified communications provides presence and point-and-click conferencing capabilities."[45] By eliminating the burdensome processes that are currently used and utilizing a UC solution users are able to collaborate on the fly. Users can also drag and drop people into the conference at will allowing everyone to participate in the same session.[46]

Implementation of Unified Communication:

The Goldwater-Nichols Act of 1986 centralized the civilian command of the military, clearly delineated the chain of command, and mandated cooperation between the services. The Goldwater-Nichols Act effectively changed how the military is structured and how the services interact with one another.[47] In the years following Goldwater-Nichols, there was still division between the services when it came to the acquisition and administration of IT assets. In order to correct the services divergent cultural adopted toward IT systems the Clinger-Cohen Act was passed. The Clinger-Cohen Act mandated the following:

> Agency heads are to design and implement processes for maximizing the value and managing the risks of their IT acquisitions. This provides for the selection of investments using minimum criteria on whether to undertake an investment and gives a means for senior management to obtain timely information on cost, capability of the system to meet requirements, timeliness and quality. IT investment processes are to be integrated with the processes for making budget, financial, and program management decisions.[48]

The DoD ensures it is in compliance with both the Goldwater-Nichols Act and the Clinger-Cohen Act; however, the DoD has fallen short of true integration and interoperability between service IT systems. There is currently no DoD enterprise level integration of communication systems. As it stands, each service and the Office of the Secretary of Defense (OSD) maintains separate and distinct networks. Collaboration between services is limited to external portal sites which do not provide a clear operational picture.

DCO and Intelink are the only two portal sites that provide inter-service collaborative capabilities. The capabilities DCO and Intelink provide are limited in scope. DCO is the more robust of the two sites. As discussed previously, DCO supports video, audio, document sharing, and desktop sharing. The problem with DCO is it is a passive system. Users must receive an invite to a session and log into the session in order to participate. Intelink is a wiki site and document repository. The only collaborative feature Intelink provides is document sharing and editing.

During deployed operations units from different services are more likely to share IT resources. Deployed units still have a discrepancy in IT system integration with different services. Following operations in the African theater Special Purpose Marine Air Ground Task Force (SPMAGTF) 12.1 submitted an after action report detailing the communication systems used for command and control. The after action report states the following:

> Information sharing and knowledge management were facilitated through a variety of collaboration tools including Microsoft Internet Relay Chat (mIRC), SharePoint, Defense Connect Online (DCO), Jabber MomentIM, and Intelink, which became the primary means and was deemed most effective[49]

Separately each system identified is capable of providing reliable Command and Control (C2) support. The issue is there is no integration between these systems. In order to access SharePoint permission must be granted. Jabber and mIRC are separate chat applications. Submitting information on one is not transcribed to the other. Managing information flow on these disjointed systems is counterintuitive to C2.

UC supports the staff officer's ability to streamline information flow. Information flow within a Command Operation Center (COC) is structured around processes established along functional areas. The identified processes do not always facilitate efficiency. Calls and emails are directed to users without the appropriate skillsets or authority to make a timely decision. UC ensures the right person, receives the right information, to make a decision.

Unified communication is a complex issue. Different organizations have different needs which shape their deployment plan. The enterprise architecture must be kept in mind when developing an implementation plan. Robert Desourdis Jr., a senior systems architect at Science Applications International Corporation, addresses this when writing, "enterprise architectures can be created at many different levels within and across governance, organizations, and jurisdictional or stakeholder boundaries, but these uses must be strongly coordinated."[50] The DoD UCMP directs the following minimum requirements for UC implementation:

> 1. Drive technology insertion through a common UC operational framework.
> 2. Transition to UC using implantation phases defined by each DoD Component, as specified in respective DoD Component implementation plans. DISA and the other DoD Components shall collaboratively integrate these implementation phases to maintain consistency and integrity of the UC operational framework, and to manage overall DoD UC risks.
> 3. Employ prototype, preproduction, multi-vendor, and UC Pilot test and evaluation activities to ensure products are interoperable, secure, and NetOps compliant.
> 4. Use competitive multi-vendor approved products based on common user requirements and listed on the DoD UC approved products list (APL).

5. Ensure Quality of Service (QoS) is available end-to-end, independent of technology employed, for non-assured/assured UC.
6. Reduce the Defense Red Switch Network (DRSN) footprint by revalidating user requirements, migrating users, as appropriate, to classified DISN voice services such as Voice over Secure Internet Protocol (VoSIP), investing in an IP capable DRSN, and enabling gateways among DoD classified voice networks
7. Provide UC across DoD and commercial networks using commercial standards, as appropriate.
8. Implement end-to-end UC at a pace consistent with respective DoD Component mission requirements and available resources. DoD Components shall coordinate with DISA on UC implementation schedules to ensure synchronization across the DoD enterprise.
9. Use the DoD identity management and access control process.[51]

The one common thread is that all UC plans require an organized and repeatable planning process. The implementation plan should follow industry best practices to ensure compatibility and future upgradeability. The end state is to develop a "robust information-sharing architecture for true interoperability."[52]

Because UC is an integration tool the sum of its parts can be modular. This allows organizations to leverage their already existing infrastructure increasing their return on investment. The IT administrator with input from key stakeholders needs to determine what features would work best for the organization. Working with the users to develop a common picture of how the architecture should function will ensure the network is functional and secure. As experts assert this vision of the architecture should include "guidance, rules, and product descriptions for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating Families of Systems (FOSs), Systems of Systems (SoSs), and interoperating and interacting architectures"[53]

In order to deploy a suitable UC solution the DoD will have to combine separate systems. Given the current budget crisis the DoD will need to get a significant return on investment (ROI) for not only current systems but any potential new system investments. A UC platform adopted by the DoD will need to be capable of integrating with the current hardware and software infrastructure while enhancing functionality. Any interoperability issues with existing hardware and software will be a nonstarter for DoD implementation.

Conclusion:

There have been significant technological advancements in the field of telecommunications. The systems alone do not amount to a revolutionary change in the way users communicate and interact, how people use those systems does. The versatility and functionality of social networking is a prime example. Users today are able to exchange thoughts and interact with other users geographically dispersed in a way unimaginable only a few years ago. This new capability is UC, a variant of social media. The integration of diverse telecommunication assets that can access different services is the foundation for a revolutionary shift in the way people interact and collaborate.[54]

The future of UC is unknown. As more organizations embrace this capability more venders will develop varying solutions. Determining the best solution for an organization is difficult. It will depend on the needs of the organization. The type of required connectivity will also play an important role. Mobile and isolated users will not only want similar capabilities, but will justifiably require similar capabilities in order to be productive.

There is currently no set standard for a unified communication platform. Designing a resilient system with the redundancy to survive an austere environment, yet flexibility enough to meet the requirements of service members will be difficult. For the US military, relying on industry best practices will be a starting point, but developing a robust military oriented implementation plan will be crucial to success.[55] According to Bern Elliot, this will "include initially focusing on a subset of unified communications functionality, ensuring that key stakeholders are involved in the planning, providing plenty of user training, conducting extended pilot periods, measuring success and failure of initial trials, and learning from early experiences and pilots."[56]

The potential UC holds for collaboration and work productivity is limitless. As the Marine Corps' budget is cut service members will have to leverage technology to meet demands.

A robust UC plan can have great effects in support of both garrison and deployed forces. By employing unified communications IT managers will be able to identify and remove redundant systems. The integrated capabilities will make users more productive and reduce IT costs; however, the ability of service members in austere environments to collaborate with service members supporting them from within the United States is priceless and it is possible through UC.

There are security concerns with UC. Those concerns can be mitigated through diligent network security practices at both the administrator and user level. All of the mitigation techniques discussed are already implemented on both garrison and tactical Marine Corps networks. UC can offer service members a "streamlined mechanism for managing communications."[57] There is no justification to avoid the usage of this technology because of a fear of vulnerabilities. With the proper implementation of security protocols and standard network security devices potential vulnerabilities can be mitigated. This will allow UC platforms to function in their intended manner.

UC is an enabler for the modern warfighter. Unified communication platforms will provide users with the ability to use the most appropriate medium of communication to collaborate with a distributed force. The users can be in garrison or forward deployed and still have the ability to collaborate in real time. This ability will significantly improve the speed at which information can be gathered, exchanged, and processed, fundamentally changing operational art. Increased productivity and functionality in the command operation center will lead to increased operational effectiveness. This effort has started and is ongoing. The challenge will be ensuring that these integrated functions are effectively implemented so that leaders have the right information at the right time and are not overwhelmed by it. The implementation of UC will provide the Department of Defense with an interoperable communications platform with disparate systems that will effectively increase the warfighter's ability to make decisions.

Illustrations

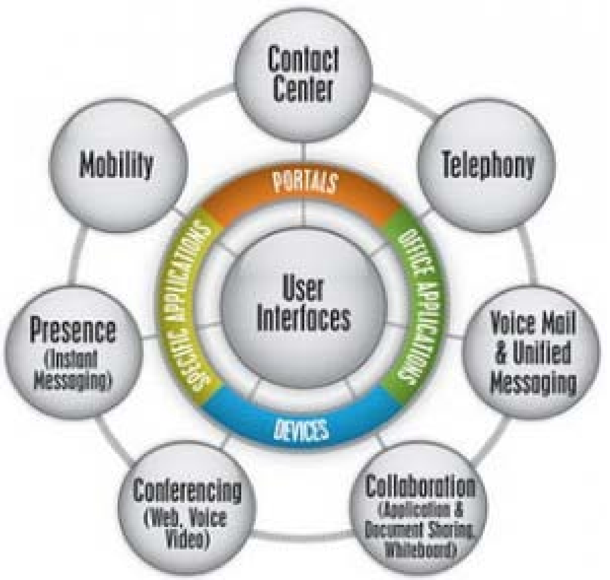
Contact Center
Telephony
Voice Mail & Unified Messaging
Collaboration (Application & Document Sharing, Whiteboard)
Conferencing (Web, Voice Video)
Presence (Instant Messaging)
Mobility
PORTALS
OFFICE APPLICATIONS
DEVICES
SPECIFIC APPLICATIONS
User Interfaces

Figure 1, unified communications diagram for business[58]

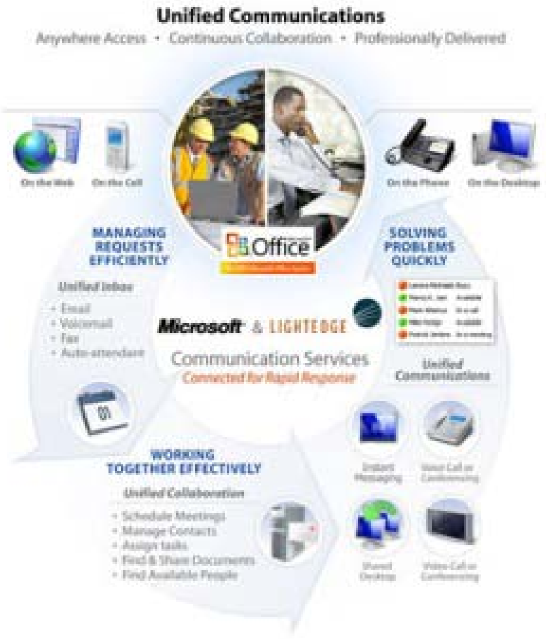

Figure 2, Communication service[59]

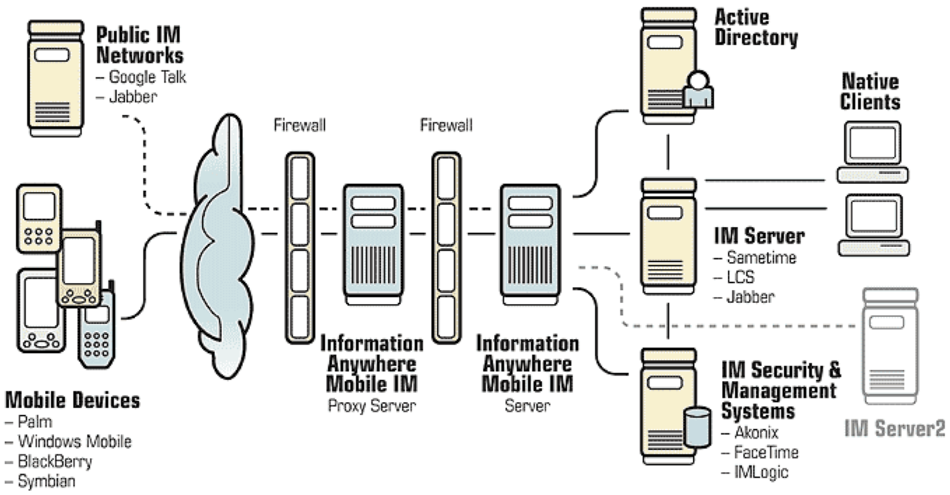

Figure 3, Mobile Instant messaging architecture[60]

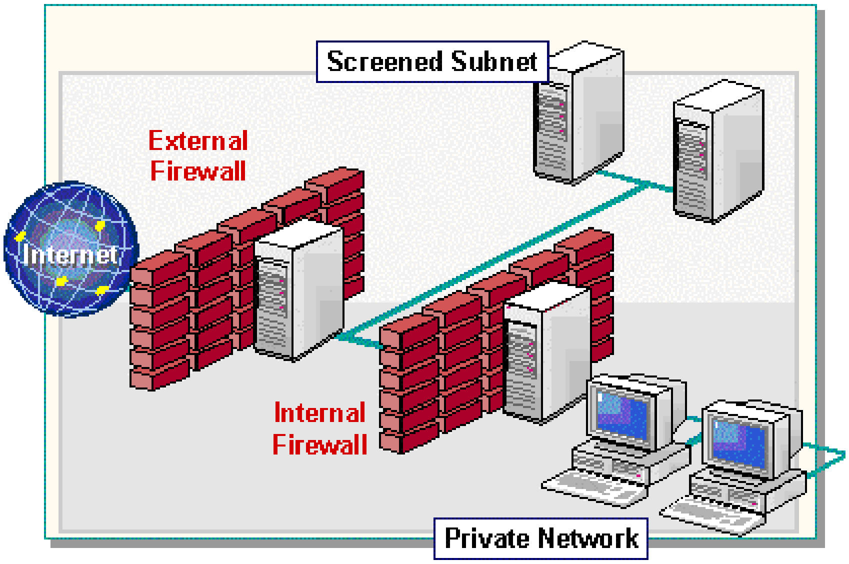

Figure 4, Network DMZ[61]

[1] Oxford Dictionaries n.d. Online, s.v. "Digital Native." http://oxforddictionaries.com/us/definition/american_english/digital%2Bnative?q=digital+native (accessed February 21, 2013).
[2] Marc Prensky, "Digital Natives, Digital Immigrants." *On the Horizon Vol 9*, No. 5, (October 2001): 2.
[3] Prensky, 2.
[4] U.S. Department of Defense, *Internet Services and Internet-based Capabilities*. Instruction 8550.01 September 11, 2012, http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf.
[5] Commandant of the Marine Corps, *Fiscal Year 2010 Responsible and Effective Use of Internet-Based Capabilities*, MARADMIN 18110, March 29, 2010, http://community.marines.mil/news/messages/Pages/MARADMIN181-10.aspx.
[6] Facebook Statement of Rights and Responsibilities, accessed 22 February 2013, http://www.facebook.com/legal/terms.
[7] Dagny Evans, "An Introduction to unified communications: challenges and opportunities," *Aslib Proceedings 56, no. 5 (*2004): 311.
[8] Bern Elliot, "The Value of Unified Communications," *Network World.com,* January 2, 2008, http://www.networkworld.com/news/tech/2008/010208-tech-update.html.
[9] Vincent Puglia, "Unified Communications: The search for ROI through tomorrow's business communication solutions," (master's thesis, Rochester Institute of Technology College of Applied Science and Technology, 2010), 6.
[10] Microsoft TechNet Library, 2013, http://technet.microsoft.com/en-us/library/aa991542.aspx.
[11] George Durzi and Michael Greenlee. *Professional Unified Communications Development with Microsoft Lync Server 2010.* (Indianapolis: Wiley Publishing, 2011), 2.
[12] Durzi and Greenlee, 2.
[13] Durzi and Greenlee, 2.
[14] Jun Xu and Mohammed Quaddus. *E-Business in the 21st Century : Realities, Challenges and Outlook* (World Scientific Publishing Co., 2009), 13.
[15] Gavin Hill, *"Securing IP telephony - Can you hear me now?,"* (White Paper, Dimension Data, 2007), 2-4.
[16] Hill, 2-4.
[17] John W. Rittinghouse and William M. Hancock, *Cybersecurity Operations Handbook* (Burlington: Digital Press, 2003), 191.
[18] Rittinghouse and Hancock, 191.
[19] Xu and Quaddus, 13.
[20] Dr. Talal Al-Kharobi and Mohmmed Abdullah Al-Mehdhar, "Comprehensive Comparison of VoIP SIP Protocol Problems and CISCO VoIP System" *International Journal of Network Security & Its Applications* 4, no. 4 (2012): 143.
[21] J. Dawkins, G. Manes, and M. Papa, A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks, *Journal of Network and Systems Management* 13, no. 3 (2005) 258.
[22] Roger Hulme, One for all: unified messaging comes of age, *International Journal of Productivity and Performance Management* 52, no. 3 (2003): 142
[23] Hill, 2-4.
[24] Chris Brenton and Cameron Hunt, *Mastering Network Security*, (Alameda: SYBEX Inc, 2003), 112.
[25] Brenton and Hunt, 112.
[26] Brenton and Hunt, 112.
[27] Brenton and Hunt, 113.
[28] Brenton and Hunt, 114-115.
[29] Brenton and Hunt, 115.
[30] Brenton and Hunt, 115.
[31] Brenton and Hunt, 115.
[32] Brenton and Hunt, 115.
[33] Brenton and Hunt, 129.
[34] Brenton and Hunt, 191.
[35] G. Camarillo, H. Schulzrinne, and R. Kantola, "Evaluation of Transport Protocols for the Session Initiation Protocol" *IEEE Network* 17, no. 5 (2003): 40-46.
[36] Rittinghouse and Hancock, 163.
[37] Rittinghouse and Hancock, 274.
[38] Rittinghouse and Hancock, 274.

[39] U.S. Department of Defense. *Unified Capabilities Master Plan*, October 2011, 17, http://www.disa.mil/Services/Network-Services/UCCO/~/media/Files/DISA/Services/UCCO/APL-Process/Unified_Capabilities_Master_Plan.pdf.
[40] Elliot, 24.
[41] Elliot, 24.
[42] Elliot, 24.
[43] Elliot, 24.
[44] Neeraj Gill, "Putting the Unified in Unified Communications - Collaboration is the Key" *Communications Today*, 2011.
[45] Forrester Consulting on Behalf of Cisco, *Unified Communications Transform Business Communication* (Cambridge: Forrester Research, Inc, 2005), 9.
[46] Forrester Consulting, 9.
[47] *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, Public Law 99-433 (1 October 1985)
[48] *Clinger-Cohen Act 1996*, Public Law 104-106 (10 February 1996)
[49] "Security Force Assistance in Support of Marine Force's: Africa's Theater Security Cooperation Campaign," 2012, Special Purpose Marine Air Ground Task Force 12.1
[50] Robert I. Desourdis et. al., *Achieving Interoperability in Critical IT and Communication Systems* (Boston: Artech House, 2009), 139.
[51] U.S. Department of Defense, 17.
[52] Desourdis, 107.
[53] Desourdis, 139.
[54] K. V. Prasad, *Principles of Digital Communication Systems and Computer Networks*, (Herndon VA: Charles River Media, 2004), 447
[55] Elliot, 24.
[56] Elliot, 24.
[57] Evans, 311.
[58] Spaulding Hill Networks, June 18, 2010, "NEC Unified Communication for Business: A Single Server Powerhouse!"
[59] Lightedge, *Unified Communications as a Service*, 2012, http://www.lightedge.com/productsservices/uc/index.html
[60] "Mobile productivity suite adds secure IM," *eWeek*, July 18, 2007, http://www.windowsfordevices.com/c/a/News/Mobile-productivity-suite-adds-secure-IM/
[61] Kenneth Pfeil, "Data Security and Data Availability in the Administrative Authority," accessed March 2, 2013, http://technet.microsoft.com/en-us/library/cc722918.aspx

Bibliography

Al-Kharobi, Dr. Talal, and Mohmmed Abduallah Al-Mehdhar. "Comprehensive Comparison of VoIP SIP Protocol Problems and CISCO VoIP System." *International Journal of Network Security & Its Applications* 4, no. 4 (July 2012): 137-152.

Brenton, Chris, and Cameron Hunt. *Mastering Network Security.* Alameda: SYBEX Inc, 2003.

Camarillo, G., H. Schulzrinne, and R. Kantola. "Evaluation of Transport Protocols for the Session Initiation Protocol." *IEEE Network* 17, no. 5 (2003): 40-46.

Clinger-Cohen Act. Public Law 104-106 (February 10, 1996).

Dawkins, J., K. Clark, G. Manes, and M. Papa. "A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks." *Journal of Network and Systems Management* 13, no. 3 (September 2005): 253-267.

Department of Defense . "Directive-Type Memorandum (DTM) 09-026 Responsible and Effective use of Internet-based Capabilities." February 25, 2010.

Department of Defense Chief Information Officer. "Department of Defense Unified Capabilities Master Plan." 2011.

Desourdis, Jr., Robert I., Peter J. Rosamilia, Christopher P. Jacobson, James E. Sinclair, and James R. McClure. *Achieving Interoperability in Critical IT and Communication Systems.* Boston: Artech House, 2009.

Durzi, George, and Michael Greenlee. *Professional Unified Communications Development with Microsoft Lync Server 2010.* Indianapolis: Wiley Publishing, Inc., 2011.

Elliot, Bern. "The Value of Unified Communications." *Network World*, Jan 2008: 24.

Evans, Dagny. "An Introduction to unified communications: challenges and opportunities." *Aslib Proceedings: New Information Perspectives*, 2004: 308-314.

eWeek. *Mobile productivity suite adds secure IM.* July 18, 2007. http://www.windowsfordevices.com/c/a/News/Mobile-productivity-suite-adds-secure-IM/.

Facebook. *Statement of Rights and Responsibilities.* 2013. http://www.facebook.com/legal/terms.

Forrester Consulting on Behalf of Cisco. *Unified Communications Transform Business Communication.* Cambridge: Forrester Research, Inc., 2005.

Gill, Neeraj. "Putting the Unified in Unified Communications - Collaboration is the Key." *Communications Today*, 2011.

Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433 (October 1, 1986).

Headquarters Marine Corps Command, Control, Communication, and Computers. "Responsible and Effective use of Internet-based Capabilities ." March 29, 2010.

Hill, Gavin. *Securing IP telephony - Can you hear me now?* White Paper, Dimension Data, 2007, 2-4.

Hulme, Roger. "One for all: unified messaging comes of age." *International Journal of Productivity and Performance Management* (MCB UP Ltd) 52, no. 3 (2003): 141-144.

Lightedge. *Unified Communications as a Service.* 2012. http://www.lightedge.com/productsservices/uc/index.html.

Microsoft. *TechNet Library* . 2013. http://technet.microsoft.com/en-us/library/aa991542.aspx (accessed February 25, 2013).

Oxford Dictionaries. *Oxford Dictionaries.* n.d. http://oxforddictionaries.com/definition/english/digital%2Bnative (accessed Feb 21, 2013).

Pfeil, Kenneth. *Data Security and Data Availability in the Administrative Authority.* 2013. http://technet.microsoft.com/en-us/library/cc722918.aspx (accessed 03 02, 2013).

Prasad, K. V. *Principles of Digital Communication Systems and Computer Networks.* Herndon, VA: Charles River Media / Cengage Learning, 2004.

Prensky, Marc. "Digital Natives, Digital Immigrants." *On the Horizon*, 2001.

Puglia, Vincent. "Unified Communications: The search for ROI through tomorrow's business communication solutions." *Rochester Institute of Technology College of Applied Science and Technology*, February 2010.

Rittinghouse, John W., and William M. Hancock. *Cybersecurity Operations Handbook.* Burlington: Digital Press, 2003.

Spaulding Hill Networks . *NEC Unified Communication for Business: A Single Server Powerhouse!* June 18, 2010. http://spauldinghillnetworks.com/blog/nec/nec-unified-for-business/.

Special Purpose Marine Air Ground Task Force 12.1. "Security Force Assistance in Support of Marine Force's: Africa's Theater Security Cooperation Campaign." After Action Report, 2012.

Symantec. *PC Tools.* n.d. http://www.pctools.com/security-news/zero-day-vulnerability/ (accessed Feb 23, 2013).

U.S. Marine Corps . "Communictions and Information Systems." *MCWP 3-40.3.* July 10, 2001.

Xu, Jun, and Mohammed Quaddus. *E-Business in the 21st Century : Realities, Challenges and Outlook.* World Scientific Publishing Co., 2009.